The shift to cyber power

TATIA MOSIDZE

Russia's invasion of Ukraine has involved the most extensive use of offensive cyber operations by one state against another in history. It is now obvious that blurring the lines between competition, crisis and war in cyberspace requires continuity in cyber defence. As a result, national cybersecurity must be one of the state's top priorities in terms of policy focus and budget allocation.

Forces that influence the world order are constantly evolving, and therefore, the global security landscape has become even more dynamic. For decades, the power dynamics of global balance were different to those today. Those with an economic advantage had the upper hand and dictated the rules to the rest of the world. Soon after, the emphasis moved towards military might, particularly during the Cold War. Of course, the economy is also the backbone here, as the development of weapons requires a strong and stable economy.

At the same time, there is no denying that military might plays a crucial role in today's world as well. However, in recent years, there has been a dramatic change in the global security landscape and along with technological competition and trade wars there is now a shift from traditional military power to cyber power. If the previous world was that of a nuclear arms race, we are today in a technological "rat race", where those who bring more innovation will be the ones dictating the rules to others.

Cyberspace and power

With the advancement of technology, countries are increasingly focusing on building their cyber capabilities to gain an edge in global affairs. Needless to say, cyber-attacks can be just as devastating, if not more so, than traditional military attacks, making cybersecurity a top priority for many nations. The world has already seen events from Stuxnet, a computer worm that was originally aimed at Iran's nuclear facilities and has since mutated and spread to other industrial and energy-producing facilities, to recent cyber-warfare in modern conflicts. With this increasing demand and as everything becomes more interconnected online, the ability to defend against cyber threats has become essential to maintaining a country's security and influence on the world stage.

While economic and military strength remain important factors in global politics, the ability to adapt and excel in the cyber domain is becoming increasingly crucial for maintaining power and influence. The emphasis on technological superiority and cyber capabilities may ultimately outweigh traditional economic and military advantages in the shaping of global politics. Cyberspace's low costs, ease of access, anonymity, vulnerability, asymmetry and other features have led to the phenomenon of power distribution. For example, a small group of hackers can disrupt the operation of a large enterprise through cyber-attacks and demonstrate how power can be wielded through digital technology. In addition, nation states can use cyber capabilities to influence elections in other countries (as allegedly Russia did in the 2016 presidential elections in the United States), highlighting the potential for asymmetric power in cyberspace.

The emphasis on cyber capabilities may ultimately outweigh traditional economic and military advantages in geopolitics.

The concept of the cyber component becoming more and more of a key pillar in national security strategies underlines its growing influence at the local, regional and international level. For example, the Office of the US Director of National Intelligence (DNI) listed cyber threats, including the development of weapons of mass destruction, as the most significant global threat to the United States. Additionally, the US Defense Department has identified cyber threats as one of the greatest challenges facing the military. US President Joe Biden acknowledged the difficulties of returning too quickly to past practices and emphasized the need for a new approach in both foreign and national security policy, as the security landscape is rapidly changing.

We can see the changing dynamic in the US's national cybersecurity strategy from last year alongside that of the defence ministry. Both strategies emphasize

the importance of partnership and collaboration: "Build Enduring Advantages in Cyberspace – The department will pursue institutional reforms to create advantages that will last for decades … ensure the availability of timely and actionable intelligence to support cyberspace operations, as well as investigate the intersection of emerging technologies and cybersecurity capabilities."

In today's world one of the biggest threats after WMD (Weapons of Mass Destruction), chemical, biological, radiological, nuclear threats, has a technological character. Now cyber capabilities are shaping a country's strength starting from national security and ending with economy.

A wake-up call

The intense and comprehensive war taking place as a result of Russia's invasion of Ukraine has made all this clear. It is the most extensive and ongoing use of offensive cyber operations by one state against another in history. It is now obvious that blurring the lines between competition, crisis and war in cyberspace requires continuity in cyber defence. As a result, national cybersecurity must be one of the state's top priorities in terms of policy focus and budget allocation. For example, in the case of the war in Ukraine, which still threatens the global security order, from the very beginning Russia has used cyber operations to disrupt critical infrastructure, such as power grids and government networks, causing widespread chaos and instability. This demonstrates the need for robust cyber defence measures to protect against such attacks and ensure national security in the digital age. A borderless domain makes it harder to be proactive, and this is one of the main reasons why a power shift is happening from nuclear weapons to cyber power. If "X" state wants to be powerful, influential and a globally dominant player then it must have advantages in cyberspace. A country's security largely depends on the reliability and security of its cyber infrastructure. Therefore, cyber-attacks can harm the country's international relations, economy, security and diplomacy. For example, in February 2021, Russian hackers attacked the Ukrainian government database and attempted to share information from a programme that installed malware on computers that downloaded data.

In a separate incident in May 2021, a North Korean hacker group conducted a cyber-espionage campaign targeting key South Korean officials. These cyber-attacks disrupted government activities and undermined relations between the two countries. These events highlight the importance of cybersecurity measures, including high-level understanding and international cooperation, to protect national interests.

Immediately following the start of Russia's invasion of Ukraine, the US, Canada, Finland, France, Germany, Japan, the Netherlands, Poland, Sweden and the United Kingdom refined or strengthened the restructuring of their militaries' cyber assets, not only for military operations but also to ensure that peacetime military elements are reinforced for continuous national cyber defence. This war served as a wake-up call for the international community to refresh their cyber arsenal.

Cyber beyond military

National cyber defence is dependent on effective partnerships between governments and the private sector, as well as alliances with countries with similar priorities. While it is important to enhance cyber-military assets in response to the Russian aggression, focusing solely on military operations may neglect other crucial aspects of national cyber defence, such as infrastructure protection and civilian cybersecurity. Furthermore, Russia's full-fledged invasion of Ukraine and the whole *modus operandi* behind it have highlighted the importance of technology companies as geopolitical actors, given their decisive interventions in the conflict.

Several cyber exercises were carried out during the war in Ukraine, indicating that military power, which has been the traditional weapon of conflict until now, will set the stage for intense cyber capabilities and new ways of modern warfare. In February 2023, France hosted ORION 23, where French and international cyber experts simulated a scenario of a cyber-attack disrupting critical infrastructure, showcasing the potential impact of cyber-warfare on modern conflicts. Around the same time, the British Army oversaw Defence Cyber Marvel 2, Western Europe's largest cyber-military exercise during which the organization tested their cyber capabilities in response to a fictional state-sponsored cyber-attack, highlighting the growing importance of cybersecurity in national defence strategies.

Access to the internet and online communication should be internationally recognized as a fundamental human right and freedom.

General Paul Nakasone, the head of US Cyber Command, confirmed for the first time that the US has carried out offensive cyber operations in support of Ukraine. Various US units, including US Navy SEALs units, were officially deployed and involved in the war to increase Ukraine's cyber capabilities. In addition to providing real-time assistance (repelling cyber incidents), they also trained local cyber specialists.

It is critical that access to the internet and communications be included as an internationally recognized fundamental human right and freedom, and that this

be a prerequisite for a new form of humanitarian intervention. Ukrainian media outlets were targeted in an attempt to crack down on state media and facilitate Russian propaganda. A prime example of this would be the spread of false information about Ukrainian government officials to undermine trust in state media.

Another example would be the use of cyber-attacks to disrupt the work of Ukrainian media outlets and prevent them from publishing accurate information. Russia targets insurance and healthcare organizations and aims to collect information on Ukrainian citizens to "support" business networks and prospective information. One detailed example is when security databases are breached and hackers steal Ukrainians' personal information, which would then be used to target them in disinformation campaigns. Another example would be the penetration of health organizations to collect information about the health of the Ukrainian population in order to create false plans about the problems of health consumption in Ukraine.

New tools, new responses

The case of Ukraine demonstrates the involvement of active cyber intervention, as attacks on energy, communications, mass media, and the private sector were openly displayed. There were also attacks targeted specifically at civilians. These attacks have had a direct impact on citizens, beginning with Telegram and progressing to other popular communication tools. These operations aim to limit access, hack accounts and infect devices.

At least 23 alleged Russian cyber-terrorist groups have been identified. All of them have carried out attacks against both the private and public sectors alongside offensive military operations. The most commonly identified groups include Gamaredon (related to the Russian FSB), Sandworm (GRU), and "independent hacktivists" who are actually state-controlled criminals.

> New threats require new mechanisms, ones that not only respond to challenges at the tactical and operational levels, but also on the strategic level.

The situation in Ukraine highlights the need for an effective humanitarian intervention in the realm of cyber. This is due to the need to isolate threats, not only for the safety of the target country's population but also for international security. This becomes even more imperative as other countries are now also facing attacks, such as Poland or the Baltic states. It is clear that Russian groups such as Armageddon are now directing attacks against other countries as well.

Today, cyber means having the potential to outperform traditional combat weapons in terms of effectiveness, coverage, availability and resonance. Furthermore, as

artificial intelligence technology quickly advances, authoritarian states and criminal organizations will gain access to even more sophisticated and powerful capabilities in a completely new domain upon which citizens, businesses and states rely.

At this point, new threats require new mechanisms, ones that not only respond to challenges at the tactical and operational levels, but also on the strategic level. It is crucial for governments and organizations to continuously adapt and enhance their cybersecurity capabilities to stay ahead of evolving threats in the digital age. In the context of international relations, this will also allow for a more effective, timely and adequate response. EE

Tatia Mosidze is the deputy head of the Information Technology Agency's policy and strategic development department within the Georgia Ministry of IDPs from Occupied Territories, Labour, Health and Social Affairs. She is also the co-founder and an instructor at the CASE Academy, which focuses on training on security-related disciplines.